FortiMail Virtual Appliance for Microsoft Azure Quick Start Guide

FORTIMAIL VIRTUAL APPLIANCE FOR MICROSOFT AZURE QUICK START GUIDE

The following section will take you through a step-by-step process in order to deploy Fortinet FortiMail on Azure.

What Is the FortiMail Security Email Gateway?

FortiMail Virtual Email Security delivers proven, powerful messaging security for any size organization or service provider. Secured by FortiGuard, FortiMail delivers the latest technologies and intelligence, including integrated sandboxing, to stop even the most sophisticated email-borne threats. Closing off this threat vector plays an important role in a cohesive approach to securing your organization against the latest attacks.

Highlights:

- Scalable solution for small and medium businesses to the largest ISP and carrier networks
- Advanced threat outbreak protection methods to protect against new, emerging, and targeted attacks
- Apply identity-based encryption in both push and pull methods
- Data leak prevention and policy-based encryption and archiving enable compliance with SOX, GLBA, HIPAA, and PCI DSS
- Enforce email and security policies at a granular level
- Receive real-time security updates from FortiGuard Services
- Multi-layer threat detection delivers highest level of user protection
- Scalable solution delivers long-term investment protection

Why FortiMail Virtual Appliance on Azure?

Stop Email Threats and Protect Sensitive Information

Email has long been a favorite attack vector of cybercriminals and is often an early stage of advanced threats. Not only do you need to keep threats from getting in, but you need to keep data from getting out. Fortinet's email security solution has the highly effective, yet easy to use inbound and outbound protection you need. It comes in a large range of offerings to fit any size organization or service provider. Plus, unmatched flexibility in deployment modes and form factors means it fits perfectly in any environment.

- Independently top-rated effectiveness: routinely earning top marks in Virus Bulletin, AV Comparatives, and other third-party testing
- Comprehensive coverage: anti-spam, anti-phishing, anti-malware, sandboxing, data loss prevention (DLP), encryption, and message archiving
- High performance: advanced software architecture for industry-leading throughput and price performance

How to Deploy the FortiMail in Microsoft Azure Using the Azure Portal and ARM

The FortiMail Security Email Gateway for Microsoft Azure is deployed as a virtual machine in Microsoft's Azure cloud (IaaS). You will see in the following sections how to deploy and configure the FortiMail in the Azure Marketplace. Fortinet solution templates and virtual machines can be found in the referenced link below.

- https://azure.microsoft.com/en-us/marketplace/partners/fortinet/
- FortiMail Security Email Gateway (BYOL)—This is currently the only licensing model that is supported. Fortinet also offers a 60-day evaluation license.

BEFORE YOU GET STARTED

Before you can begin to deploy the FortiMail Security Email Gateway Virtual Appliance, you will need to make sure the following conditions have been met in order to successfully complete the installation:

- Create a Microsoft Azure account
- Obtain a license

Either:

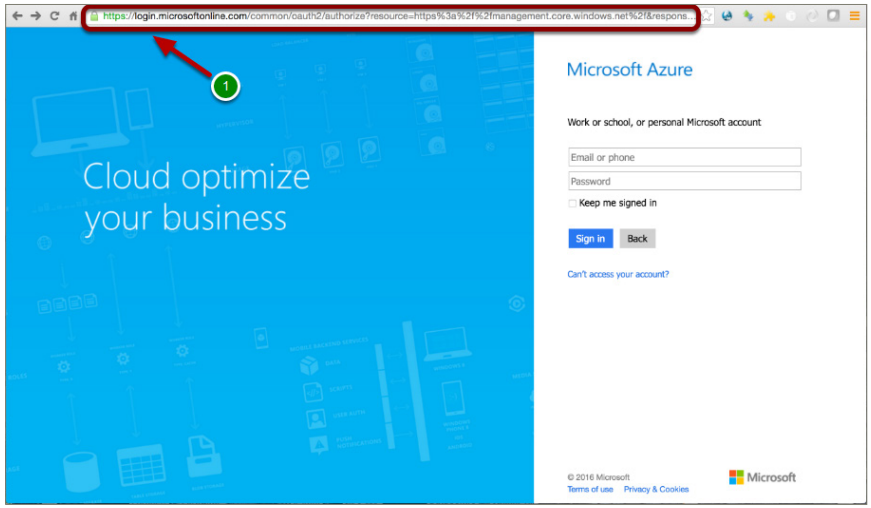
1. Purchase a FortiMail Security Email Gateway license for Microsoft Azure http://www.windowsazure.com/en-us/account/
2. Register to receive an evaluation license from Fortinet https://support.fortinet.com/Evaluation/Login.aspx

Step-by-Step Instructions to get the FortiMail Security Email Gateway Virtual Appliance Up and Running on Azure

The following section will take you through a step-by-step process in order to deploy a Single Instance FortiMail Security Email Gateway Virtual Appliance on Microsoft Azure.

1. Log In to the Azure Portal
   - You can access the Azure portal using the following URL: https://portal.azure.com/
   - You will be redirected to a login page if currently not already logged in.
   - You will then be redirected to the portal dashboard.

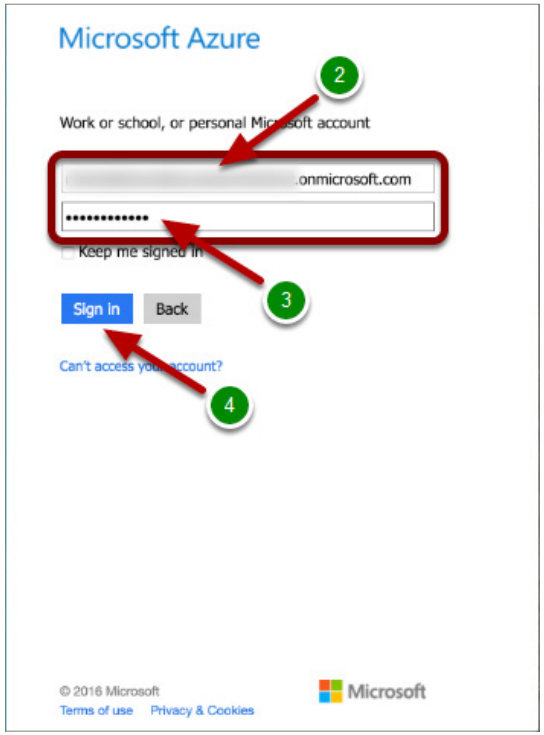
   The current Azure portal is the portal through which you will start creating and managing Azure services. The Azure portal includes a dashboard that you can configure to work with and monitor the resources in your environment. The Azure portal lets you administer all of your Azure platform resources in a single location. The current Azure portal uses Azure Resource Manager (ARM), although some classic model functionality is exposed through the new portal. The legacy or classic portal still is available for use, but the new portal has been released for general availability and is the portal you should use.



2. Enter User Credentials and Sign In

   Enter your user credentials:

   - Username: <Your Username> (2)
   - Password: <Your Password> (3)
   - Click "Sign in." (4)

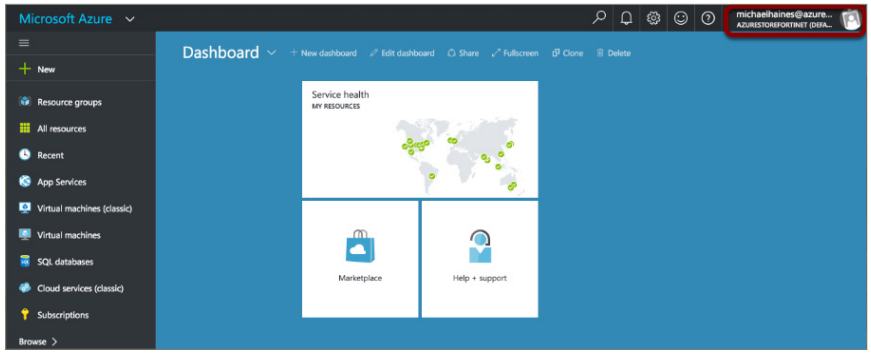


3. Successful Login to Azure

   Once you have successfully logged in to the Azure portal, you will observe the Microsoft Azure Dashboard.

   Note the following login details in the top right-hand corner of the Microsoft Azure Dashboard. If you click here, you will see options to:

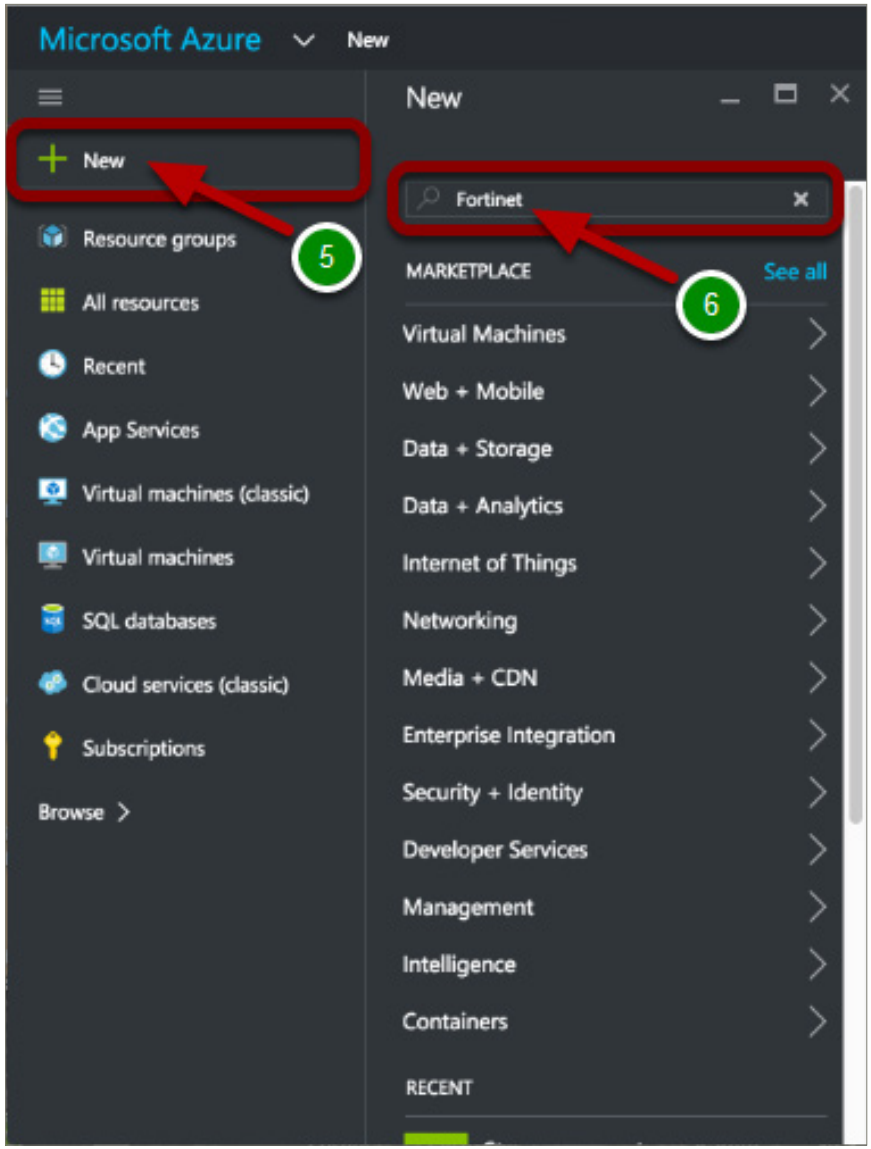
   - Sign out
   - Change your password
   - View your permissions
   - View your bill



4. Creating the NEW FortiMail VM in the Azure Marketplace

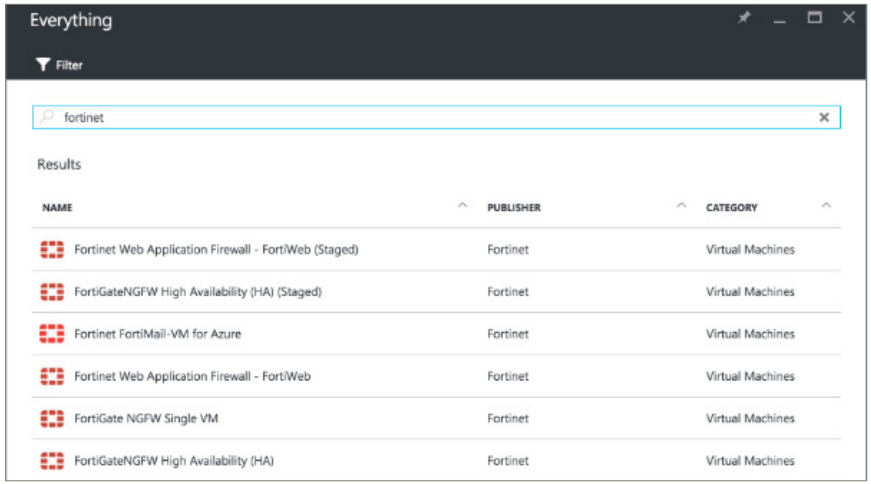
   In the Microsoft Azure portal, follow these steps:

   - In the upper left-hand corner, click New (5).
   - In the New column, enter Fortinet in the "search the marketplace" and press "Enter" (6).



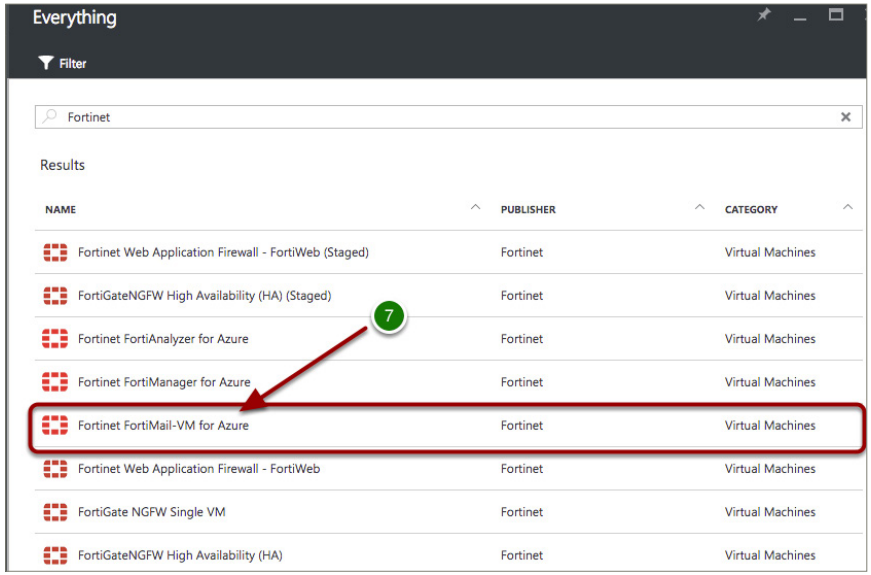
5. Fortinet Virtual Appliances Available in the Azure Marketplace

   You will now see something similar to this, which depicts the return of the "Fortinet" search results.



6. Select the FortiMail-VM from the Azure Marketplace

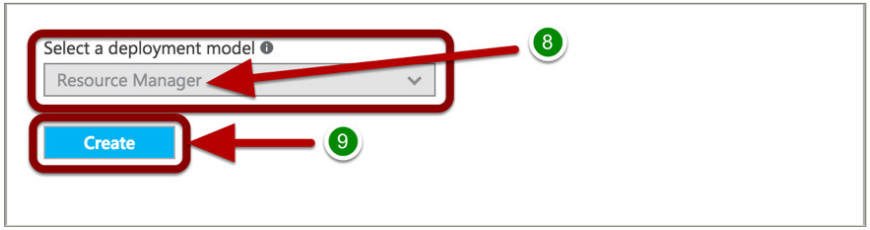
   Select Fortinet FortiMail-VM for Azure (7).



7. Select the FortiMail VM Deployment Model

   Once you have selected the FortiMail-VM, you will automatically be taken to the Resource Manager Panel, where you can create a deployment model.

   - In the Select a deployment model, select the default Resource Manager (8).
   - Then click Create (9).



NOTE: Though there is no option from the dropdown menu to select a different deployment model, this is where you would select the Classic deployment model option.

So what exactly are the Azure deployment models?

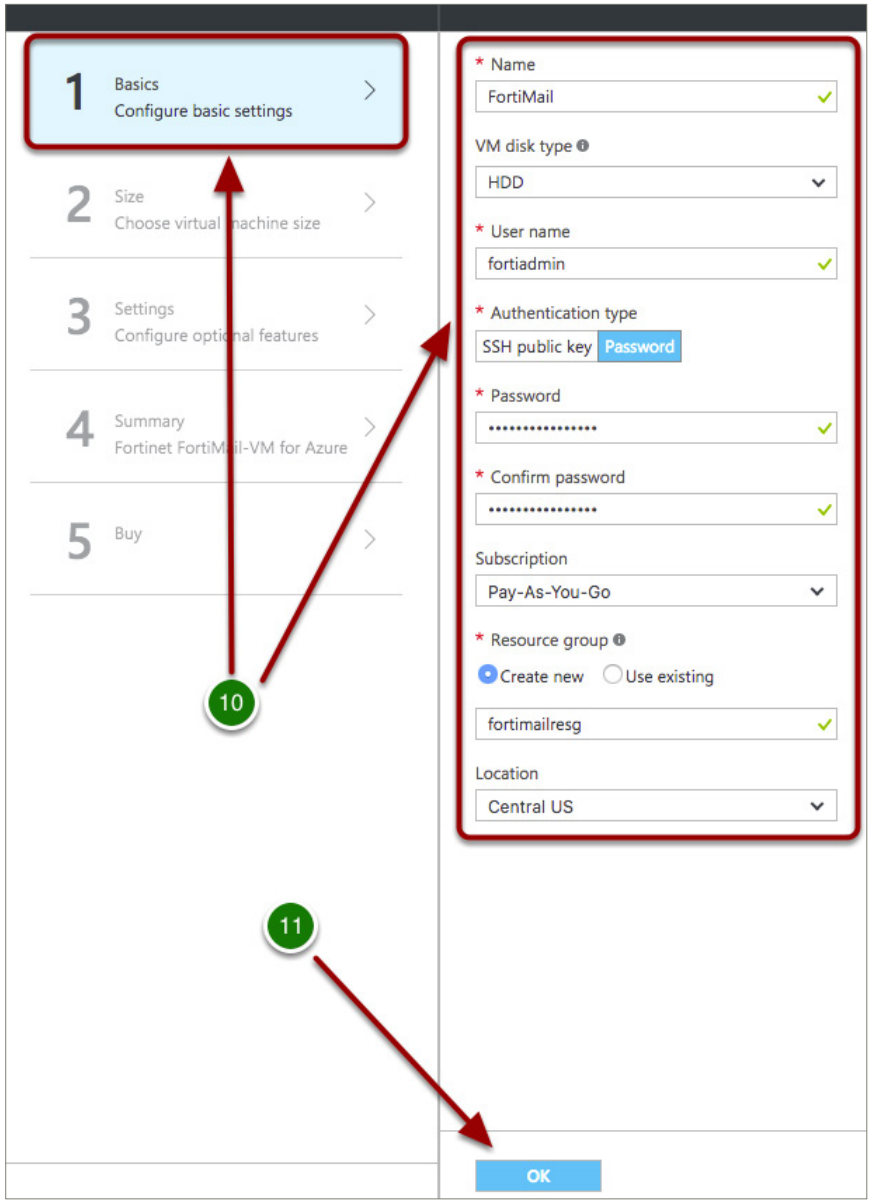
Azure provides two deployment models, the Classic model and the Azure Resource Manager (ARM) model. The foundation of each model is an application-programming interface (API), which is the Resource Manager API for ARM and the Service Management API for the classic model. Although developers can write software to interact with these APIs directly through the REST API, it is more common to interact with these APIs indirectly using the Azure portal, the Azure PowerShell on Windows, or the Azure Command-Line Interface (CLI) on a Windows, OS X, or Linux computer.

In contrast to common belief, these two models are compatible with each other, but ARM simplifies the deployment and management of resources by managing them as a single resource group. Most newer resources support ARM, and eventually all resources will. However, how you create, configure, and manage Azure resources is different in these two models.

8. Configuring the FortiMail VM Basic Settings

   In the Configure basic settings panel (10), enter:

   - **FortiMail VM Name**—Enter the name of the FortiMail Virtual Appliance. (Only alphanumeric characters are permitted, and the value must be between 1 and 15 characters.)
   - **FortiMail Administrative Username**—Enter the administrator username for the FortiMail Virtual Appliance. (The administrator username for the FortiMail Virtual Appliance can NOT be "admin".) If you do enter "admin," you will get an error message stating that the specified username is NOT allowed. In addition to this, the username can NOT contain special characters.
   - **Authentication type**—Change Authentication type to Password.
   - **FortiMail Password**—Enter the administrator account password for the FortiMail Virtual Appliance. (The administrator account password MUST be between 6 and 72 characters, and MUST contain characters from at least three of the following groups: uppercase characters, lowercase characters, numbers, and special characters.)
   - **Confirm password**—Re-enter the administrator account password for the FortiMail Virtual Appliance.
   - **Subscription**—The only available subscription for the FortiMail Virtual Appliance in Azure is the Pay-As-You-Go subscription model, so just leave this as the default.
   - **Resource group**—Enter the Resource group name, and note that only alphanumeric characters, periods, underscores, hyphens and parentheses may be used. In addition to this, a Resource group name can NOT end with a "." (With Azure Resource Manager, everything you provision on Azure is a resource. You can put multiple resources into a resource group. Managing resource groups and creating and updating resource groups are the most common operations using Azure Resource Manager.)



- **Location**—Select a location from the drop-down menu. The location refers to allowing you to administer all of your Azure platform resources in a single location.

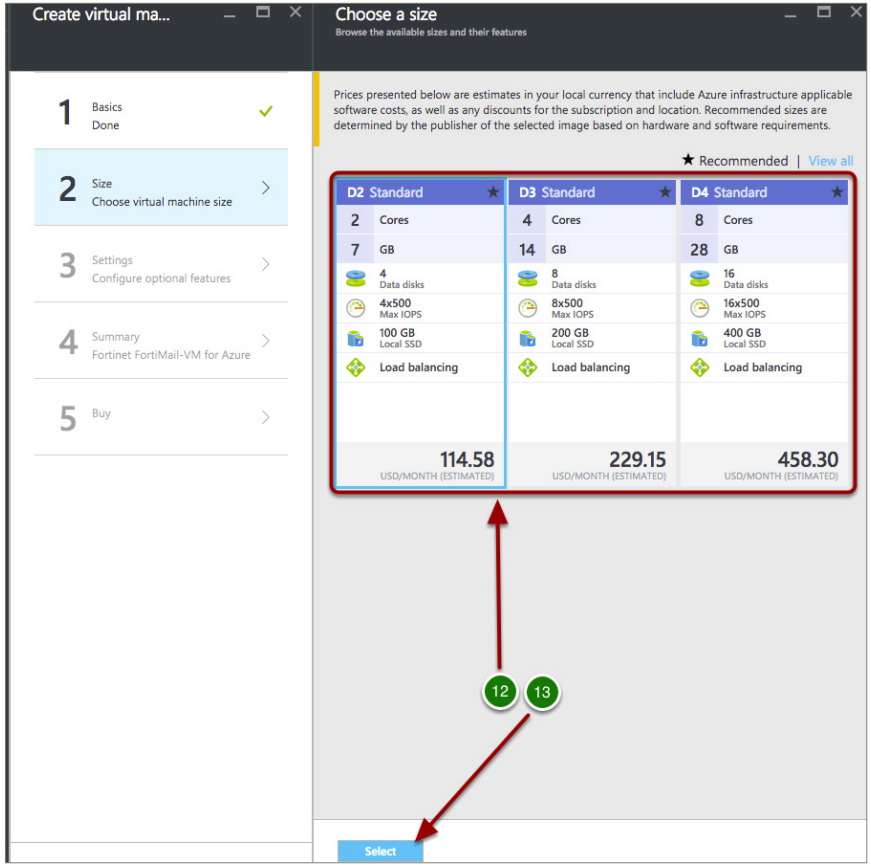
Once you have confirmed that all the above settings are correct, click "OK" (11).

NOTE: If any of the values are incorrectly defined, you will see a "Red **!**"; otherwise, you will see a "Green ✓."

9. Configuring the FortiMail VM Size

In the Choose virtual machine size panel, select the appropriate size VM for the deployment case (12). To minimize cost in a test environment, select the smallest recommended instance, as pictured here, that is D2 Standard. There are both larger and smaller instances that can be selected if View all is clicked to change the view. It is, however, not recommended to provision an instance smaller than what is outlined within the recommended sizes.

After selecting an instance size, click Select (13).

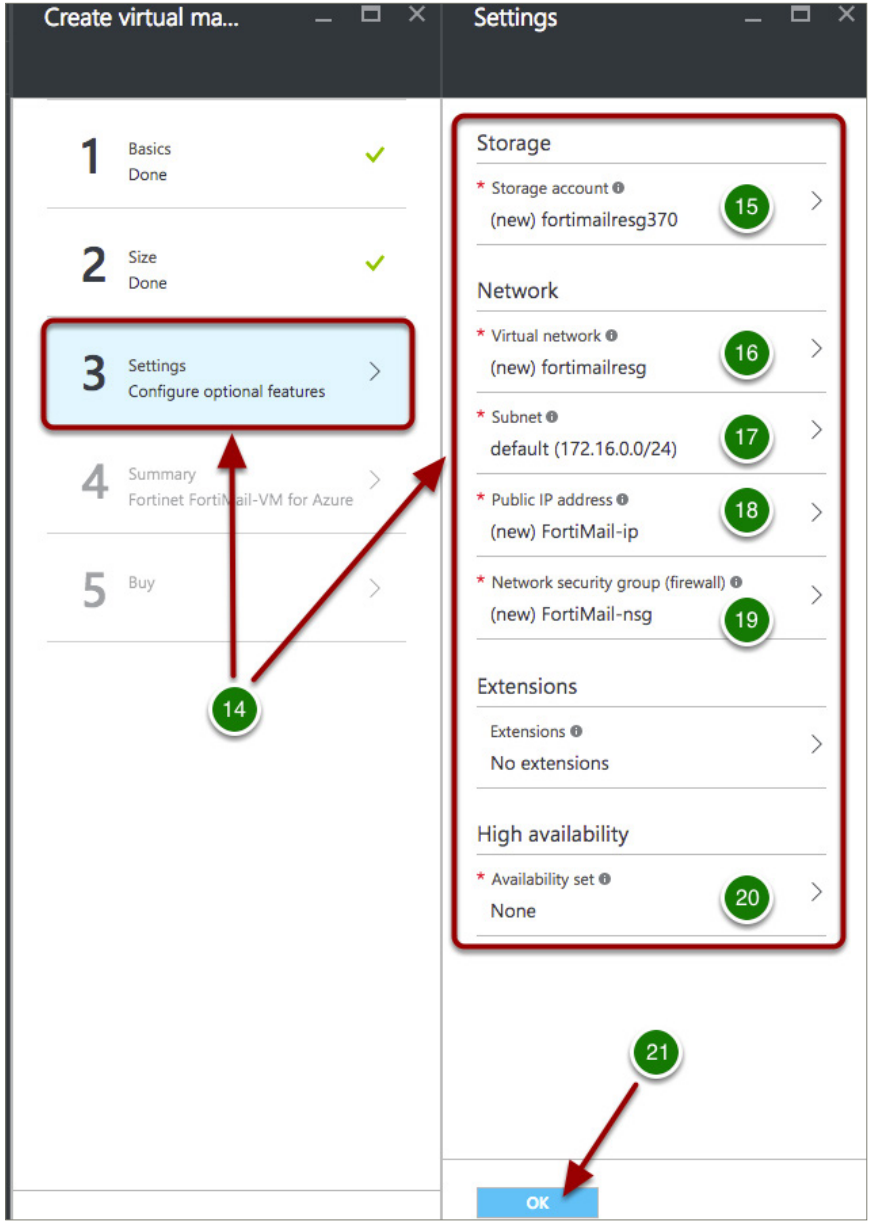


10. Configuring Optional FortiMail VM Settings

You will now be in the Configure optional features section. This contains prepopulated and dynamically named sections that do not need to be modified unless your deployment is to cohabitate preexisting resource group components including storage (15), virtual network/VNET (16), subnet (17), public IP address (18), network security group (19), or availability set (20).

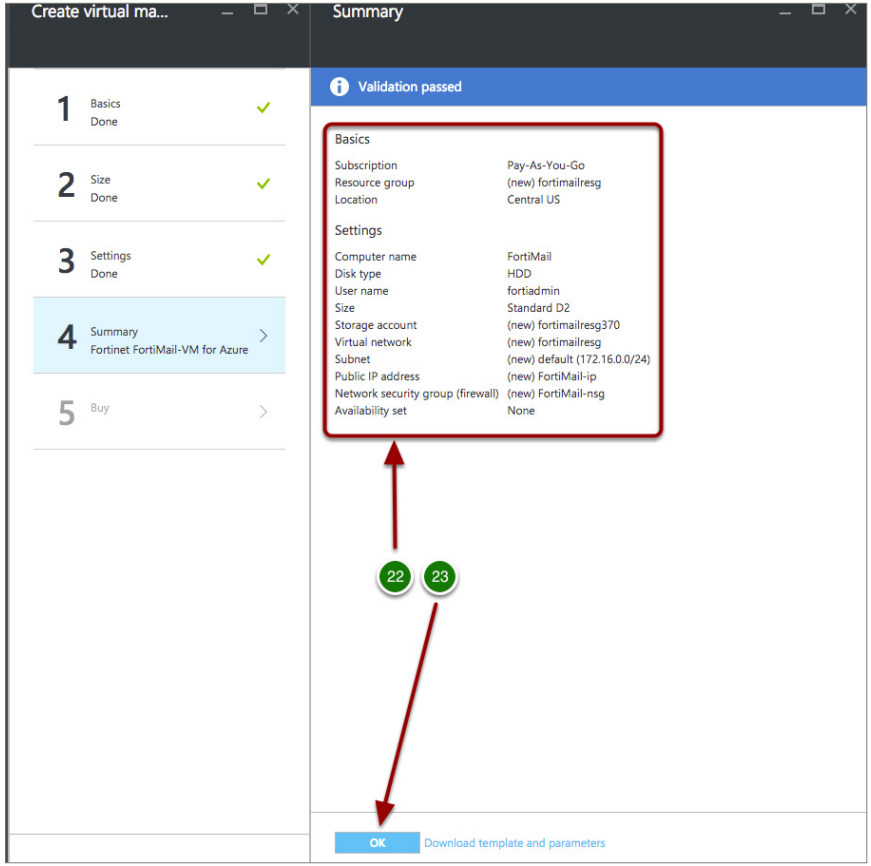
The sections that would often be modified to fit into an existing topology, within or across resource groups, would be contained in the networking portion. However, since you are deploying the FortiMail VM as a single instance on its own, there is no need to change default values. Look for additional Fortinet documentation and guidance on advanced deployments of cooperative products.

Click OK (21) and accept the default values.



11. Summary Review for FortiMail VM Deployment

    Since no values were changed in the Settings section, the next step within the process should pass validation and present a summary of what will be created (22). All new components are preempted with (new). Click OK (23) to continue to purchase review within the Buy section.

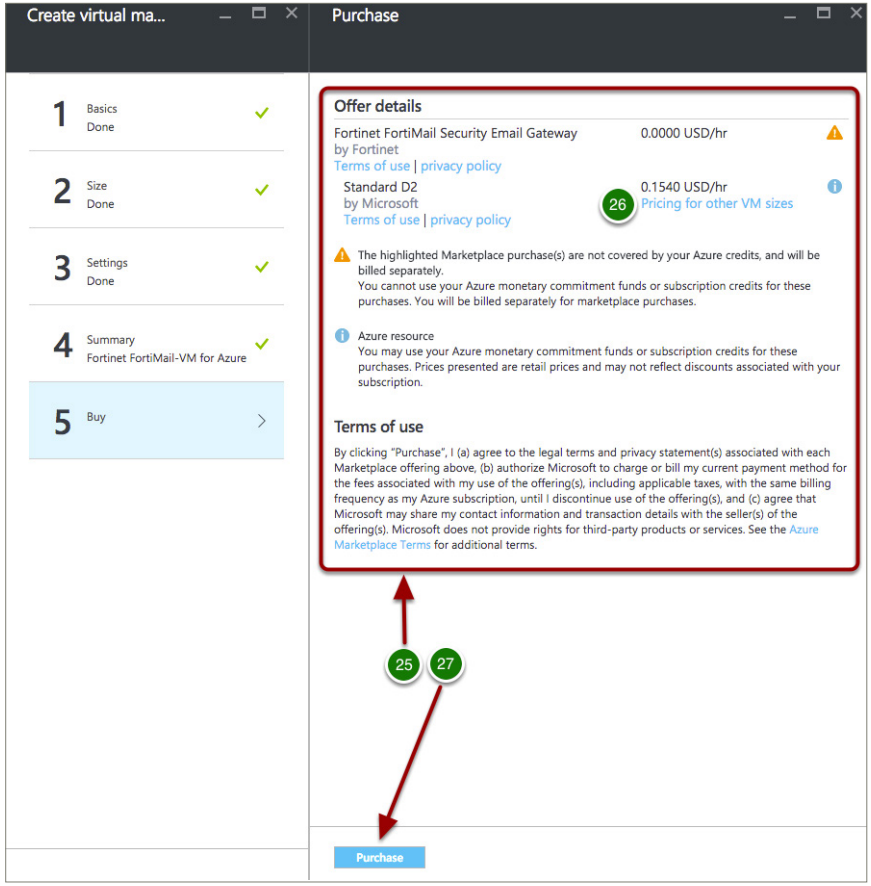


12. FortiMail VM Purchase

After the FortiMail Security Email Gateway configuration has been completed, you are now required to select Purchase. Please review the details and terms of service outlined (25). This section will inform you if Azure credits are applicable for components. Also, there is an option to compare pricing for other VM sizes within this section (26).

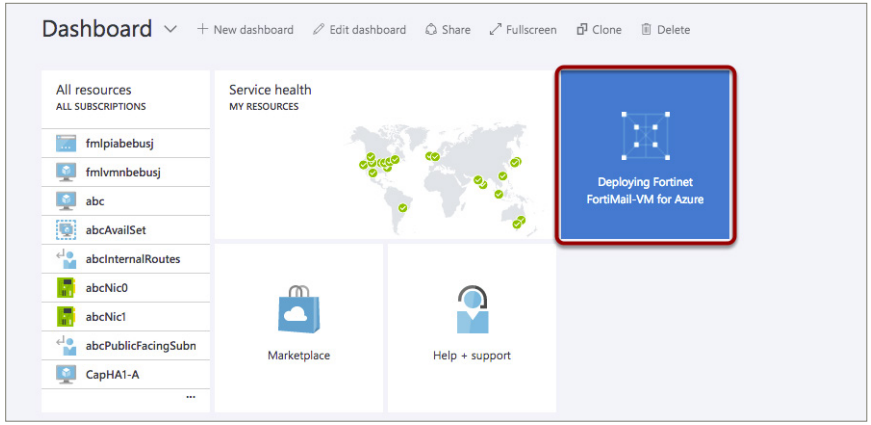
Select Purchase (27) to deploy.

NOTE: Purchase means that you are going to be paying Azure for the virtual machine use time. You still must obtain a license separately from Fortinet, Inc.



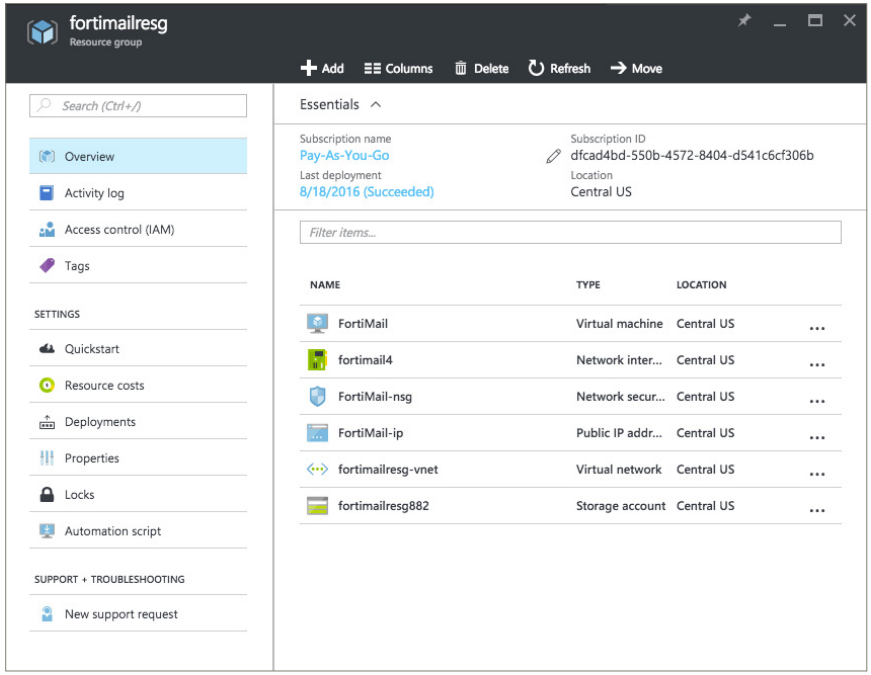
13. FortiMail VM Deployment

After selecting “Purchase,” the FortiMail VM will be deployed. This process can take approximately 10 minutes to complete, but may vary depending on location and number of resources being requested.



14. FortiMail VM Post-Deployment Validation

After the FortiMail VM has been deployed, you will be redirected to a screen similar to this that shows all the resources that have been instantiated by the template. This is the Resource Group view of what was deployed and is searchable by name within the Azure portal.

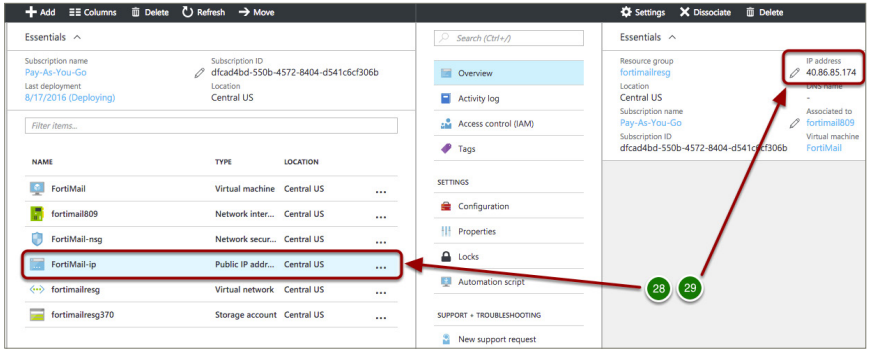


15. FortiMail VM Public IP Address

In order to be able to connect to the FortiMail VM, you need to know what the public IP address is.

To accomplish this:

Select the public IP resource (28) to get your DNS name or public IP address. This will expose the public IP address (29), which is 40.86.85.174 in this example.



16. Connect to the FortiMail VM GUI (HTTPS)

To validate that the FortiMail VM in Azure is working, you can connect to the GUI using HTTPS.

Using a modern browser such as Firefox or Chrome, connect to the IP address identified in the previous step. In this example the IP is: 40.86.85.174.

Browse to the administrative URL for the FortiMail VM. With regard to our example IP, ours will be as follows:

https://40.86.85.174/admin/ (30)

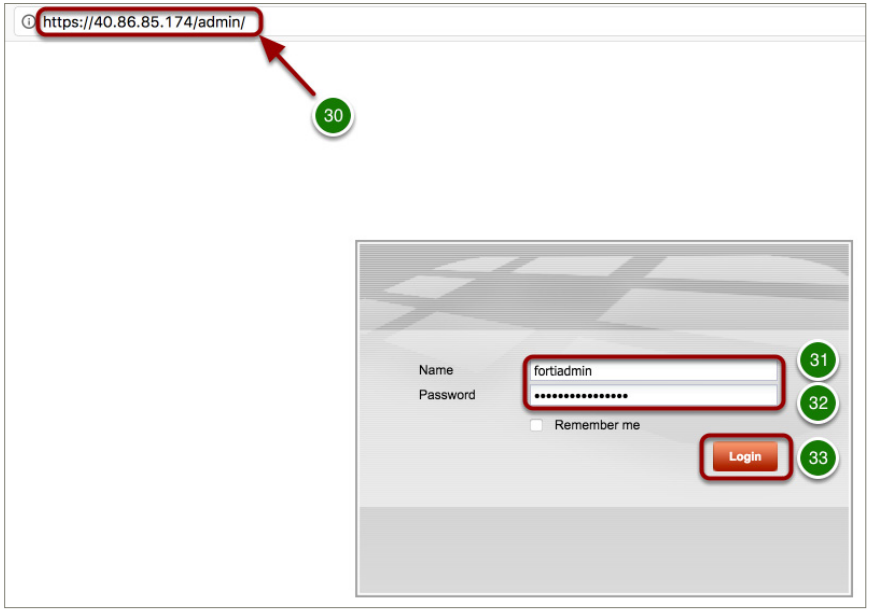
NOTE: FAILING TO SUPPLY THE ADMIN (/admin) LINK WILL PRESENT THE USER INTERFACE AND LOGIN WILL FAIL!

Enter the FortiMail Administrative Username from Step 8 (31).

Enter the FortiMail Administrative Password from Step 8 (32).

Select Login (33).

Browsing to the administrative GUI insecurely (port 80/non-HTTPS) will result in a redirect. Also be aware the default certificate is self-signed and you will receive a browser error until a valid certificate is configured.



17. License Your Azure FortiMail VM

Upon a successful login, you will be redirected to the main dashboard.

Currently our Azure Marketplace deployment only supports BYOL licenses. This means you will need to purchase Azure-specific licenses for the appliance you are going to deploy or request trial licensing from your local Fortinet or partner sales team.

NOTE: If you have a mismatch between the VM size and the license (i.e., more CPUs assigned to the VM than are licensed), you will receive an error message and the FortiMail licensing will fail until an appropriate license type is uploaded.

To license the VM, select Update from the VM license section (34).

NOTE: To obtain a license file, you will need to submit a valid registration code to the Asset section of Fortinet Support. This will then allow you to download the appropriate license file.

Once the appropriate license has been uploaded, the GUI will now reflect a valid license and you will have successfully deployed FortiMail VM in Azure. Please reference the configuration and operation documentation to configure FortiMail.

http://docs.fortinet.com/fortimail/admin-guides

Support

For more in-depth instructions, please refer to http://docs.fortinet.com/ for administration guides or email your support questions to azuretech@fortinet.com.

v1.0 09.07.16